DATA PROCESSING AGREEMENT - CONTRATTO PER LA NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI
AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679

Il presente Accordo sul Trattamento dei Dati Personali ("DPA") viene stipulato tra FRACTALGARDEN S.r.l., con sede legale in via Residenza Sassi 1 - 20054 Segrate (MI) in persona del suo legale rappresentante (di seguito il "Responsabile del Trattamento") e il CLIENTE (di seguito il "Titolare del Trattamento"),

di seguito anche denominati singolarmente come "Parte" e congiuntamente come "Parti".

PREMESSO CHE:

- in virtù del contratto stipulato tra le Parti o dell'adesione al servizio "OTP service" il Responsabile del Trattamento si assume l'obbligo di fornire al Titolare del Trattamento i servizi di cui all'Allegato del presente DPA;
- in relazione al trattamento dei dati personali connesso all'erogazione dei Servizi, entrambe le Parti si impegnano al rispetto di tutti gli obblighi specificatamente previsti dalle leggi vigenti italiane ed europee sulla protezione dei dati personali, ed in particolare il D.Lgs 196/2003 ("Codice in materia di protezione dei dati personali") così come da ultimo modificato dal D.Lgs. 101/2018, e il Regolamento (UE) 2016/679 (di seguito anche "Gdpr");
- riguardo a tale trattamento, ai sensi dell'art. 28 del Gdpr, Fractalgarden S.r.l., agisce in qualità di Responsabile del Trattamento dei dati personali di cui il Cliente è Titolare del Trattamento. I dati personali saranno trattati dal Responsabile del Trattamento esclusivamente al fine dell'esecuzione dei Servizi come descritti nell'Allegato e per il tempo strettamente necessario all'esecuzione degli stessi, nel rispetto delle istruzioni fornite dal Titolare del Trattamento;
- qualora le Parti abbiamo regolato il rapporto per mezzo di un contratto di adesione al servizio "OTP service", queste convengono che il presente DPA costituisce un *Addendum* e quindi è parte integrante e sostanziale di tale contratto.

CIO' PREMESSO, le Parti convengono quanto segue:

1. Definizioni

Si riportano di seguito alcune definizioni utili al fine di facilitare la corretta comprensione del presente documento:
Addendum: Documento integrativo che viene allegato a un contratto o accordo già esistente, al fine di modificarne o integrarne determinate disposizioni, senza la necessità di redigere un nuovo contratto.
Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.
Autorizzati al trattamento: si tratta di persone fisiche che, sotto l'autorità diretta del Titolare o del Responsabile del Trattamento, sono autorizzate a trattare i dati personali agendo in base alle istruzioni fornite dal Titolare o Responsabile rispettando il principio di confidenzialità e le misure di sicurezza stabilite.
Cliente: si tratta di un una persona fisica o un'organizzazione che acquista, utilizza o beneficia del servizio OTP service erogato da Fractalgarden S.r.l.
Consultazione preventiva: processo mediante il quale un'organizzazione consulta l'Autorità Garante per la protezione dei dati personali prima di avviare un trattamento dei dati che potrebbe comportare un rischio elevato per i diritti e le libertà delle persone fisiche.
Dato personale: qualsiasi informazione relativa a una persona fisica identificata o identificabile ("Interessato"). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, mediante un identificativo quale il nome, numero di identificazione, dati relativi all'ubicazione, identificativo online o uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
GDPR: si riferisce al Regolamento Generale sulla Protezione dei Dati (UE) 2016/679.
Impatto: rappresentazione del grado di gravità dell'incidente che comporta compromissione della riservatezza, integrità e disponibilità dei trattamenti e dei dati ad essi relativi.
Interessato: persona fisica a cui si riferiscono i dati personali.
Luogo di processamento: si riferisce alla regione selezionata da Fractalgarden S.r.l. per l'archiviazione dei dati personali del Cliente, all'interno di un data center. Le regioni in cui sono situati i data center disponibili sono esclusivamente all'interno del territorio europeo.
Minaccia: evento potenziale, cagionato ovvero accidentale che comporterebbe un danno all'interessato.
Normative sulla Protezione dei Dati: comprendono le leggi e i regolamenti che regolano il trattamento dei dati personali e stabiliscono obblighi per i soggetti che trattano tali dati, al fine di proteggere i diritti alla privacy e alla sicurezza delle persone fisiche, garantendo che i dati siano trattati in modo lecito, corretto e trasparente.
Paese Terzo: si tratta di un paese situato al di fuori dell'UE (Unione Europea) o dello Spazio Economico Europeo (SEE), non riconosciuto dalla Commissione Europea come avente un livello di protezione dei Dati Personali adeguato ai sensi dell'art. 45 GDPR.
Probabilità: valutazione della frequenza con la quale si verifica una minaccia funzionalmente alle vulnerabilità presenti e delle eventuali misure di contenimento adottate.
Responsabile del trattamento: la persona fisica/giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (si tratta di un soggetto esterno all'organizzazione).

Rischio: è uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità per i diritti e le libertà. Il rischio in questa procedura è sempre riferito all'interessato.
Sub Responsabile: si tratta di soggetti terzi che vengono coinvolti dal Responsabile del Trattamento per eseguire attività specifiche relative al trattamento dei dati personali, in nome e per conto del Titolare del Trattamento.
Titolare del trattamento: la persona fisica/giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
Trattamento: qualsiasi operazione o insieme di operazioni effettuate con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, quali la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'utilizzo, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Violazione dei Dati Personali: indica una violazione della sicurezza che porta alla distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati.
Vulnerabilità: elemento di debolezza presente all'interno del sistema informativo o informatico sfruttabile dalla minaccia per la produzione del danno.

2. Termini relativi al Trattamento dei Dati

2.1. Nel corso della fornitura dei Servizi al Titolare del Trattamento, il Responsabile del Trattamento può trattare i dati personali per conto del Titolare secondo i termini del presente DPA.

2.2. Nella misura richiesta dalle Leggi sulla Protezione dei Dati applicabili, il Responsabile del Trattamento dovrà ottenere e mantenere tutte le autorizzazioni e permessi necessari per il trattamento dei dati personali, compresi i dati personali inerenti al presente accordo.

2.3. Il Responsabile del Trattamento manterrà tutte le misure tecniche e organizzative per soddisfare i requisiti stabiliti dal presente DPA ed altri eventuali allegati.

3. Comunicazione dei Dati

3.1. Il Responsabile al Trattamento tratta i dati personali del Titolare del Trattamento solo ai fini dell'esecuzione dell'incarico ricevuto. Il Responsabile del Trattamento non deve trattare, trasferire, modificare, correggere o alterare i dati personali del Titolare del Trattamento o divulgare o consentirne la divulgazione a terzi se non in conformità alle istruzioni documentate del Titolare del Trattamento, a meno che il trattamento non sia richiesto dall'UE e/o dalle leggi dello Stato Membro a cui è soggetto il Responsabile e/o una qualsiasi legislazione anche sovranazionale a cui è soggetto il Responsabile. Il Responsabile del Trattamento dovrà, nella misura consentita da tali leggi, informare il Titolare del Trattamento di tali requisiti legali prima di trattare i dati personali e attenersi alle istruzioni del Titolare del Trattamento per ridurre al minimo, per quanto possibile, l'ambito della divulgazione.

4. Affidabilità e Non–Divulgazione

4.1. Il Responsabile del Trattamento adotterà misure ragionevoli per garantire l'affidabilità di qualsiasi Addetto che possa avere accesso ai dati personali interessati dal trattamento.

4.2. Il Responsabile del Trattamento garantisce che tutti gli Addetti:

4.2.1. Siano informati della natura confidenziale dei dati personali trattati per conto del Titolare del Trattamento e siano a conoscenza degli obblighi del Responsabile del Trattamento;

4.2.2. Siano in possesso di formazione/certificazioni appropriate in relazione al Gdpr o qualsiasi altra formazione/certificazione richiesta dal Titolare del Trattamento;

4.2.3. Siano soggetti a impegni di riservatezza o obblighi professionali o normativi di riservatezza;

4.2.4. Siano soggetti all'autenticazione dell'utente e alle procedure di accesso quando accedono ai dati personali del Titolare del Trattamento in conformità al presente DPA o al contratto stipulato tra le Parti e alle Leggi sulla Protezione dei dati applicabili.

5. Sicurezza

5.1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile del Trattamento mette in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio che comprendono, tra le altre, se del caso:

5.1.1. la pseudonimizzazione e la cifratura dei dati personali;

5.1.2. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

5.1.3. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali del Titolare del Trattamento in caso di incidente fisico o tecnico;

5.1.4. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

5.2. Nel valutare l'adeguato livello di sicurezza, il Responsabile del Trattamento tiene conto in special modo dei rischi presentati dal trattamento, ed esplicitati nell'Allegato, che derivano in particolare dalla distruzione, dalla perdita, dalla

modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

5.3. Maggiori dettagli sulle misure tecniche ed organizzative per la protezione dei dati personali vengono riportate nell'allegato al punto 4.

6. Catena di Responsabilità

6.1. A partire dalla data di validità del presente DPA, il Titolare del Trattamento autorizza il Responsabile del Trattamento a coinvolgere altri Sub-Responsabili.

6.2. Il Responsabile del Trattamento dovrà:

6.2.1. Fornire al Titolare del Trattamento i dettagli completi sul trattamento dei dati da parte di altri Sub-Responsabili.

6.2.2. Effettuare un'adeguata due diligence su ciascun Sub-Responsabile aggiunto per garantire che possa fornire il livello di protezione dei dati personali del Titolare del Trattamento, incluse, ma non limitatamente a, sufficienti garanzie per mettere in atto misure tecniche e organizzative appropriate in modo tale che il trattamento soddisfi i requisiti del Gdpr, il presente DPA e quanto dichiarato nell'Allegato.

6.2.3. Su richiesta, il Responsabile del Trattamento dovrà fornire al Titolare del Trattamento una copia dei suoi accordi con altri Sub-Responsabili, per la sua revisione.

6.2.4. Se e quando il trattamento che consegue all'erogazione dei servizi comporti il trasferimento dei dati personali del Titolare del Trattamento al di fuori del Unione Europea, il Responsabile del trattamento dovrà incorporare le clausole di riservatezza o qualsiasi altro meccanismo attuato per garantire l'adeguata protezione dei dati personali del Titolare del Trattamento trasferiti.

6.2.5. Rimanere pienamente responsabile nei confronti del Titolare del Trattamento per qualsiasi mancanza da parte di ciascun altro Sub-Responsabile nell'adempiere ai propri obblighi in relazione al trattamento dei dati personali del Titolare del Trattamento.

7. I Diritti degli Interessati

7.1. Tenuto conto della natura del trattamento, il Responsabile del Trattamento assisterà il Titolare del Trattamento implementando le misure tecniche e organizzative appropriate, se e quando possibile, per l'adempimento dell'obbligo del Titolare del Trattamento di rispondere alle richieste degli interessati di esercitare i propri diritti come stabilito nel Gdpr dell'UE.

7.2. Il Responsabile del Trattamento dovrà informare tempestivamente il Titolare del Trattamento se riceve una richiesta da un interessato, dall'Autorità di controllo e / o altra autorità competente ai sensi delle leggi sulla protezione dei dati applicabili in relazione ai dati personali del Titolare del Trattamento.

7.3. Il Responsabile del Trattamento dovrà cooperare come richiesto dal Titolare del Trattamento per consentire:

7.3.1. La fornitura di tutti i dati richiesti dal Titolare entro un ragionevole periodo di tempo specificato dal Titolare in ciascun caso, comprese le informazioni complete e le copie del reclamo, della comunicazione o della richiesta e qualsiasi dato personali che il Titolare del Trattamento conserva relativo a un interessato.

7.3.2. Ove applicabile, fornire l'assistenza richiesta dal Titolare del Trattamento per consentirgli di soddisfare la relativa richiesta entro i termini prescritti dalla legge. Il Responsabile del Trattamento si riserva il diritto di addebitare al Titolare del Trattamento i costi ragionevoli derivanti dalla prestazione di tale assistenza, calcolati sulla base dei tempi impiegati e dei materiali utilizzati.

7.3.3. Implementare eventuali misure tecniche e organizzative aggiuntive che possano essere ragionevolmente richieste dal Titolare del Trattamento per consentire di rispondere in modo efficace a reclami, comunicazioni o richieste pertinenti.

8. Violazione dei Dati Personali

8.1. Il Responsabile del Trattamento dovrà inviare una notifica al Titolare del Trattamento senza indebito ritardo e, in ogni caso, entro ventiquattro (24) ore dall'essere venuto a conoscenza o aver ragionevolmente sospettato di una violazione dei dati personali. Il Responsabile del Trattamento fornirà al Titolare del Trattamento informazioni sufficienti per consentire al Titolare del Trattamento di adempiere a qualsiasi obbligo di segnalare una violazione dei dati personali ai sensi delle Leggi sulla Protezione dei Dati. Tale notifica deve come minimo:

8.1.1. Descrivere la natura della violazione dei dati personali, le categorie e il numero dei soggetti interessati, nonché le categorie e il numero di registrazioni di dati personali colpite dalla violazione;

8.1.2. Comunicare il nome e le informazioni di contatto del Responsabile della protezione dei dati o di altri contatti rilevanti dai quali possono essere ottenute ulteriori informazioni;

8.1.3. Descrivere il rischio stimato e le probabili conseguenze della violazione dei dati personali;

8.1.4. Descrivere le misure adottate o proposte per gestire la violazione dei dati personali.

8.2. Il Responsabile del Trattamento dovrà cooperare con il Titolare del Trattamento e intraprendere le misure ragionevoli per assistere nelle indagini, nella mitigazione e risoluzione di ogni violazione.

8.3. Il Responsabile del Trattamento potrà addebitare al Titolare del Trattamento costi ragionevoli, calcolati su base orarie e per i materiali utilizzati, per qualsiasi assistenza fornita in relazione ad una violazione di dati personali, salvo che il Responsabile del Trattamento sia ritenuto responsabile per l'evento che ha determinato l'intervento.

8.4. In caso di violazione dei dati personali, il Responsabile del Trattamento non deve informare terzi senza prima ottenere il consenso scritto del Titolare del Trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del Trattamento. In tal caso, il Responsabile del Trattamento dovrà informare il Titolare del Trattamento circa tale obbligo giuridico, fornire una copia della notifica proposta e considerare eventuali commenti formulati dal Titolare del Trattamento prima di notificare la violazione dei dati personali.

9. Valutazione d'Impatto sulla Protezione dei Dati e Consultazione Preventiva

9.1. Il Responsabile del Trattamento fornirà al Titolare del Trattamento un'assistenza ragionevole per qualsiasi valutazione d'impatto sulla protezione dei dati richiesta dall'articolo 35 del Gdpr e previa consultazione con qualsiasi autorità di controllo da parte del Titolare del Trattamento che sia richiesta ai sensi dell'articolo 36 del Gdpr, in ogni caso unicamente in relazione al trattamento dei dati personali del Titolare del Trattamento da parte del Responsabile del Trattamento.

9.2. Il Responsabile si avvale della possibilità di attribuire dei costi aggiuntivi ragionevoli su base oraria e secondo il materiale utilizzato per l'assistenza di un eventuale valutazione d'impatto sulla protezione dei dati.

10. Cancellazione o restituzione dei Dati Personali

10.1. In caso di richiesta di cancellazione o restituzione dei dati personali da parte del Titolare del Trattamento, il Responsabile del trattamento dovrà prontamente e, in ogni caso, entro e non oltre 30 giorni dare seguito alla richiesta. Dovrà inoltre:

10.1.1. Restituire una copia completa di tutti i dati al Titolare del Trattamento stesso mediante trasferimento sicuro di file nel formato indicato dal Titolare del Trattamento, cancellare in modo sicuro tutte le altre copie dei dati personali elaborati dal Responsabile del Trattamento;

10.1.2. Cancellare in modo sicuro tutte le copie dei dati personali del Titolare del Trattamento trattati dal Responsabile del Trattamento o da qualsiasi sub Responsabile autorizzato e, in ogni caso, fornire una certificazione scritta al Titolare del Trattamento attestante che ha rispettato pienamente i requisiti della sezione cancellazione o restituzione dei dati personali del Titolare del Trattamento;

10.1.3. Se richiesto dal Titolare del Trattamento cessare i trattamenti dei dati personali effettuati per conto dello stesso;

10.1.4. Se richiesto dal Titolare del Trattamento risolvere l'Accordo o il contratto eventualmente in essere (tale scelta deve essere notificata al Responsabile del Trattamento per iscritto).

10.2. Il Responsabile del Trattamento può conservare i dati solo nella misura e per il periodo richiesto dalla legge dell'Unione o dello Stato Membro, e sempre a condizione che il Responsabile del Trattamento garantisca la riservatezza di tutti i dati personali e assicuri che gli stessi siano trattati esclusivamente secondo le necessità per gli scopi specificati nelle leggi dell'Unione o degli Stati membri che richiedono la sua conservazione e per nessun'altra finalità.

11. Diritti di audit

11.1. Il Responsabile del Trattamento dovrà mettere a disposizione del Titolare del Trattamento, su richiesta, tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del Trattamento o da un altro soggetto da questi incaricato di qualsiasi sede in cui il trattamento di dati personali del Titolare del Trattamento abbia luogo. Il Responsabile del Trattamento consentirà al Titolare del Trattamento o ad altro auditor incaricato di ispezionare, verificare e copiare tutte le registrazioni, processi e sistemi pertinenti in modo che il Titolare del Trattamento possa accertarsi che le disposizioni del presente DPA siano rispettate. Il Responsabile del Trattamento dovrà fornire piena collaborazione al Titolare del Trattamento in relazione a tali audit e fornirà, su richiesta, evidenza del rispetto degli obblighi previsti. Il Responsabile del Trattamento dovrà immediatamente informare il Titolare qualora, a suo parere, un'istruzione ai sensi della presente sezione Audit (Diritti di Audit) violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

12. Trasferimento dei Dati Personali del Titolare del Trattamento

12.1. Il Responsabile del Trattamento non tratterà i dati personali del Titolare del Trattamento né consentirà a nessun Sub-Responsabile autorizzato di trattare i dati personali in un paese terzo, salvo che tale trattamento non sia espressamente autorizzato per iscritto dal Titolare del Trattamento nei confronti di determinati destinatari situati in paesi terzi.

13. Condizioni generali

13.1. Le Parti concordano che il presente Addendum cesserà automaticamente in caso di risoluzione del contratto stipulato tra Responsabile del Trattamento e Titolare del Trattamento o al termine dell'erogazione del servizio.

13.2. Qualsiasi obbligo imposto al Responsabile del Trattamento ai sensi del presente DPA in relazione al trattamento dei dati personali sopravviverà a qualsiasi risoluzione o scadenza di questo.

13.3. Se le Parti hanno regolato il rapporto mediante stipula di un contratto, il presente Addendum è regolato dagli articoli di legge previsti nel contratto stesso e per tutto il tempo in cui tali articoli facciano parte della legislazione di uno Stato membro dell'Unione Europea.

13.4. Qualsiasi violazione di questo DPA costituirà una violazione sostanziale del contratto stipulato.

13.5. Qualora una qualsiasi disposizione di questo Addendum fosse non valida o inapplicabile, il resto di questo documento rimarrà valido e in vigore. La clausola non valida o inapplicabile sarà (i) emendata se necessario per garantirne la validità e l'applicabilità, preservando allo stesso tempo il più strettamente possibile le intenzioni delle Parti o, se ciò non fosse possibile, (ii) interpretata in modo tale che la parte non valida o inapplicabile non sia mai stata contenuta in esso.

13.6. In caso di conflitto tra le disposizioni contenute nel contratto si specifica che il presente Addendum prevarrà per quanto riguarda gli obblighi relativi alla protezione dei dati delle parti.

ALLEGATO

1. ELENCO DELLE PARTI

Titolare/i del Trattamento: Cliente
Dati aziendali:
Firma e data di adesione_____

Responsabile/i del Trattamento: Fractalgarden S.r.l.
Dati aziendali: p.iva e C.F. IT05006700966 con sede legale in via residenza Sassi 1, 20054 Segrate (MI)
Firma e data di adesione: _____

Per richiedere una copia sottoscritta del presente DPA si prega di scrivere all'indirizzo supporto@otpservice.io

2. DESCRIZIONE DEL TRATTAMENTO

Nome del trattamento dei dati:
Il servizio otpservice.io realizzato da Fractalgarden S.r.l., propone in utilizzo uno strumento innovativo di sottoscrizione dei documenti informatici mediante Firma Elettronica Avanzata (FEA) e di Firme Elettroniche Semplici (FS).

Tipologie di dati personali e categorie di interessati

- Tipologie di Dati Personali:
  - Dati personali comuni e particolari inclusi nelle pratiche caricate dal Cliente e contenuti nelle pratiche sottoscritte tramite il servizio di OTP service
- Categorie di Interessati:
  - Utenti firmatari delle pratiche inviate dal Cliente

Finalità del trattamento
Fractalgarden S.r.l., tratta i dati personali degli interessati per conto del Titolare per le seguenti finalità:

- consentire all'interessato di fruire dei servizi OTP service e permettere la sottoscrizione dei documenti;
- tenuta delle pratiche sottoscritte.

3. ELENCO DEI SUB- RESPONSABILI DEL TRATTAMENTO

Fractalgarden S.r.l., potrà avvalersi dei seguenti sub-fornitori:

Ragione sociale	Tipo di service provider/ servizio erogato	Luogo di processamento
Amazon Web Services	Cloud Service Provider	EU - Irlanda
Twillio	SMS provider	USA
Subito SMS	SMS provider	Italia

4. MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

4.1. Controllo accessi e misure per identificazione e autorizzazione del personale di Fractalgarden S.r.l.

Fractalgarden S.r.l., ha implementato un sistema avanzato di controllo degli accessi per garantire che solo il personale espressamente autorizzato possa accedere ai dati personali. L'accesso a tali dati è limitato esclusivamente al personale che necessita di trattarli per finalità di supporto, e viene regolato mediante un sistema di controllo accessi basato su ruoli, che consente l'accesso esclusivamente ai dati strettamente necessari per l'espletamento delle specifiche attività di supporto.

Fractalgarden S.r.l., adotta una serie di misure per garantire l'identificazione e l'autorizzazione degli utenti, tra cui l'autenticazione degli utenti, l'autenticazione a due fattori e l'autorizzazione basata sui ruoli. Ogni utente è tenuto a utilizzare credenziali uniche per l'accesso, e l'accesso ai dati personali è concesso in base al ruolo e al livello di autorizzazione assegnato, assicurando che gli utenti possiedano l'accesso solo ai dati necessari per l'espletamento delle proprie mansioni.

Tutti gli account utente sono costantemente monitorati e vengono effettuate revisioni periodiche dei privilegi di accesso per garantire che solo le persone debitamente autorizzate possano accedere ai dati personali. Eventuali attività sospette o tentativi di accesso non autorizzato sono prontamente rilevati, segnalati e gestiti in conformità con le procedure interne di sicurezza.

Tutto il personale di Fractalgarden S.r.l., autorizzato ad accedere ai dati personali riceve formazione specifica in materia di protezione dei dati personali, al fine di garantire la conformità alle normative applicabili, ed è vincolato da un obbligo di riservatezza permanente, esteso anche al periodo successivo alla cessazione del rapporto di lavoro.

4.2. Crittografia e pseudonimizzazione dei dati

Fractalgarden S.r.l., adotta misure avanzate di crittografia e pseudonimizzazione per proteggere i dati personali da accessi non autorizzati, divulgazioni indebite o distruzioni. Fractalgarden S.r.l., impiega tecnologie di crittografia all'avanguardia per garantire la protezione dei dati sia durante il loro trasferimento (in transito) che, mentre sono conservati (in archivio), assicurando un elevato livello di sicurezza.

4.3. Archiviazione e conservazione dei dati

Fractalgarden S.r.l., si impegna a garantire che i dati del Cliente siano archiviati e conservati in modo sicuro. I dati dei clienti sono separati logicamente dai dati di sistema, delle applicazioni e da altri dati di clienti, mediante l'adozione di adeguati meccanismi di controllo e monitoraggio degli accessi. L'efficacia delle misure tecniche e organizzative adottate per garantire la sicurezza del trattamento viene testata e valutata regolarmente.

Fractalgarden S.r.l., ha implementato misure per assicurare la disponibilità e l'accesso ai dati personali in caso di incidenti fisici o tecnici.

In aggiunta a tali misure, Fractalgarden S.r.l., mantiene piani di disaster recovery e continuità operativa, appositamente progettati per garantire una risposta rapida ed efficace in caso di interruzioni o guasti. Tali piani includono procedure dettagliate per il ripristino dell'accesso ai dati personali.

4.4. Sicurezza fisica

Fractalgarden S.r.l., adotta misure appropriate per garantire la sicurezza fisica dei luoghi in cui vengono trattati i dati personali. L'accesso a tali luoghi è limitato esclusivamente al personale autorizzato.

4.5. Efficacia delle misure tecniche e organizzative

Fractalgarden S.r.l., testa, valuta e monitora regolarmente l'efficacia delle misure tecniche e organizzative adottate per garantire la sicurezza del trattamento dei dati personali.

Fractalgarden S.r.l., rivede, valuta e aggiorna periodicamente le proprie politiche e procedure per garantire che rimangano adeguate ed efficaci.

Fractalgarden S.r.l., mantiene piani di risposta agli incidenti e di continuità operativa, al fine di garantire una risposta rapida ed efficace in caso di incidenti di sicurezza o altri eventi perturbatori.

4.6. Configurazione del sistema

Fractalgarden S.r.l., implementa misure per garantire la sicurezza e l'integrità dei propri sistemi e processi, inclusa la configurazione del sistema e le impostazioni predefinite. L'azienda adotta le migliori pratiche e gli standard di settore per assicurare che i sistemi siano configurati in modo sicuro e che le configurazioni predefinite non generino vulnerabilità.

Fractalgarden S.r.l., revisiona regolarmente le impostazioni di configurazione del sistema per garantire che siano in linea con le politiche e le procedure di sicurezza aziendali. Vengono inoltre mantenuti controlli rigorosi sulle modifiche alle impostazioni di configurazione, assicurando che tutte le modifiche siano documentate, approvate e testate prima dell'implementazione.

Inoltre, i processi di sviluppo software di Fractalgarden S.r.l., includono pratiche di codifica sicura e l'azienda valuta e aggiorna regolarmente le proprie configurazioni predefinite per garantire che siano sicure e non introducano vulnerabilità potenziali.

4.7. IT interno

Fractalgarden S.r.l., ha implementato misure per garantire che la propria governance e gestione della sicurezza IT siano allineate alle migliori pratiche e agli standard di settore. L'azienda ha stabilito un quadro di governance della sicurezza IT che include politiche, procedure e controlli per assicurare la sicurezza e l'integrità continua dei propri sistemi e processi.

Fractalgarden S.r.l., revisiona regolarmente il proprio quadro di governance della sicurezza IT per garantire che rimanga aggiornato ed efficace. Ciò include la conduzione di valutazione dei rischi periodica per identificare potenziali rischi e vulnerabilità di sicurezza e l'implementazione di controlli adeguati a mitigarli.

Inoltre, Fractalgarden S.r.l., organizza sessioni di formazione sulla consapevolezza della sicurezza per tutto il personale, per assicurare che siano adeguatamente informati sui potenziali rischi di sicurezza e sulle modalità per mitigarli. I programmi di formazione coprono una vasta gamma di tematiche, tra cui la sicurezza delle password, la prevenzione del phishing e il trattamento sicuro dei dati.

4.8. Misure per garantire l'eliminazione dei Dati Personali

Fractalgarden S.r.l., riconosce l'importanza di garantire l'eliminazione dei dati personali quando non sono più necessari o su richiesta del soggetto interessato. L'azienda ha implementato misure per assicurare che tutti i dati personali siano eliminati in modo sicuro ed efficace dai propri sistemi e processi al termine dell'erogazione del servizio e/o dell'eventuale contratto stipulato fra le Parti.

Fractalgarden S.r.l., ha stabilito linee guida e procedure chiare per la gestione delle richieste di eliminazione, assicurandosi che i dati personali vengano eliminati o anonimizzati in modo sicuro quando non sono più necessari per gli scopi per cui sono stati raccolti. Ciò include l'adozione di metodi e strumenti di eliminazione sicuri per garantire che i dati personali vengano distrutti permanentemente e non possano essere recuperati.